UNITED STATES DISTRICT COURT

for the

District of Delaware

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

information associated with [redacted] that is stored at premises controlled by Apple

Case No. 22- 122M

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1201	Kidnapping

See affidavit in support of search warrant.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Charles Neagle, Jr.
Applicant's signature

Charles A. Neagle, Jr., Special Agent, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 04/13/2022

Judge's signature

City and state: Wilmington, Delaware

Hon. Sherry R. Fallon, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Charles A Neagle Jr, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account, [redacted], (hereinafter the "TARGET APPLE ID") that is stored at premises owned, maintained, controlled, or operated by Apple Inc. ("Apple"), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California 95014. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed since October of 2019. I am currently assigned to the Wilmington, Delaware Residence Agency within the Baltimore Field Division. I have a bachelor's degree in History from Virginia Tech. I am a graduate of the FBI New Agent Training Program in Quantico, Virginia. As part of my duties, responsibilities, and training, and in the course of my investigative experience, I have become familiar with the statutes, rules, regulations, policies, and procedures relating to the FBI's investigation of potential violations of federal law. As a Federal Agent, I am authorized to investigate violations of federal law and to execute warrants issued under the authority of the United States.

3. I am presently engaged, and have previously participated in, criminal investigations

focused on extraterritorial kidnappings of United States citizens. I have also been trained on violations of Title 18, United States Code, Section 1201 (Kidnapping).

4. The facts in this affidavit come from my own personal observations, training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter. It does not, however, withhold any information that would be necessary to a determination of probable cause.

5. Based on the facts set forth in this affidavit, I submit that there is probable cause to believe that the phone number [redacted] (hereinafter "the TARGET TELEPHONE"), was used by unknown suspects to facilitate violations of Title 18, United States Code, Section 1201 (Kidnapping) (hereinafter the "TARGET OFFENSE"). There is also probable cause to believe that the TARGET TELEPHONE is connected to the TARGET APPLE ID, and that both belong to the victim of the TARGET OFFENSE. There is further probable cause to believe that the TARGET APPLE ID contains evidence, instrumentalities, contraband, and/or fruits of the TARGET OFFENSE, and may lead to the identification of the individuals engaged in the commission of the offense. There is thus probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of the TARGET OFFENSE, as further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

THE TARGET OFFENSE

7. Title 18, United States Code, Section 1201 provides, in pertinent part:

> (a) Whoever unlawfully seizes, confines, inveigles, decoys, kidnaps, abducts, or carries away and holds for ransom or reward or otherwise any person, except in the case of a minor by the parent thereof, when –
>
> > (1) the person is willfully transported in interstate or foreign commerce, regardless of whether the person was alive when transported across a State boundary, or the offender travels in interstate or foreign commerce *or uses the mail or any means, facility, or instrumentality of interstate or foreign commerce in committing or in furtherance of the commission of the offense* . . . .
>
> shall be punished by imprisonment for any term of years or for life . . . . (emphasis added).

STATEMENT OF PROBABLE CAUSE

8. The victim of the TARGET OFFENSE ("the Victim") is a Delaware resident but is from Nigeria. On March 28, 2022, the Victim traveled to Nigeria to raise money and make funeral arrangements for his mother, who died in January 2022. When he arrived in Nigeria, the Victim's family made known the fundraising efforts, as well as the progress of those efforts, i.e. how much money they had raised. The Victim was staying in a small, rural village and thus everyone knew he was there. As of April 3, 2022, the Victim had raised approximately 11 million Naira, which is approximately $26,264.

9. On April 3, 2022, the Victim was at his brother's residence in Nigeria and was standing outside. While there, two vehicles pulled up to the residence and blocked in the Victim's vehicle. A male got out of the vehicle with a firearm and shot it into the air. The suspects took the Victim, used his hat to cover his face, and placed him into one of the vehicles. The Victim's wife ("the Wife") was

informed of the incident on April 4, 2022 by her brother, who lives in Nigeria and was contacted by the Victim's brother and informed of the kidnapping. The Wife had remained in Delaware.

10. On April 5, 2022, at approximately 4:00 a.m.[1], the Wife received a phone call from the TARGET TELEPHONE, which she recognized as the Victim's phone number. The male voice on the line, however, was not the Victim. The voice demanded 30 million Naira in exchange for the Victim's release. The Wife told the caller that she could only get 1.5 million Naira and would need more time.

11. At approximately 9:36 a.m. the same day, the Wife received another call from the TARGET TELEPHONE in which the kidnappers again asked about the money. She advised that she needed more time but only had access to 1.5 million. After that conversation, the Wife did not receive another call from the kidnappers.

12. At approximately 10:30 a.m. the same day, April 5, the Victim's sister ("the Sister") received a phone call from the TARGET TELEPHONE. The Victim's sister resides in Texas. She heard a male voice on the line but did not recognize it as the Victim's voice. The unknown subject demanded 30 million Naira in exchange for the release of the Victim. The caller informed the Sister that the Wife could only get 1.5 million Naira and that was not enough. The Sister told the caller that she could get 10 million Naira. The caller then lowered the demand to 20 million Naira. The Sister requested to speak to the Victim, but the caller hung up. Approximately 10 minutes later, the Sister received another call from the TARGET TELEPHONE. This time, the Sister recognized the Victim's voice on the line and was able to confirm that he was alive. The kidnappers then came back on the line and told the Sister that she had until 2:00 p.m. that day to pay the money. The kidnappers advised they would call her back to arrange the payment.

[1] All times stated herein are Eastern Daylight Time, unless otherwise specified.

13. At approximately 12:39 p.m. the same day, the Sister received another call from the TARGET TELEPHONE. An unknown male voice stated that they would accept 15 million Naira. The Sister agreed to that price, and they arranged for a family member in Nigeria to drop off the money. The suspects advised that if any law enforcement showed up to the exchange, they would shoot and kill the Victim. The suspects then advised that they would contact the Sister early the next morning when the banks opened to arrange the money exchange. The Sister requested to speak with the Victim again, but the suspects hung up and did not return the phone call.

14. The next morning, April 6, 2022, the Sister received a phone call from the TARGET TELEPHONE to arrange the payment. She requested again to speak with the Victim before she agreed to the exchange. The Sister spoke with the Victim and ultimately agreed to the facilitation of the money drop. The family member in Nigeria dropped 12 million Naira (approx. $28,812) at the designated location in Nigeria and observed three males pick up the money. The family member sat alone in her car waiting for the Victim to be released, but when it got dark, she left the area.

15. Later that day, at approximately 6:30 p.m., the Victim contacted his wife via the TARGET TELEPHONE and advised that he was released and staying with family in his home village.

16. In an interview after he was released, the Victim advised that the TARGET APPLE ID belongs to him and that it is associated with the TARGET TELEPHONE.

17. On or about April 11, 2022, investigators issued a letter to Apple to preserve information associated with the TARGET APPLE ID for the dates of April 3, 2022 through April 7, 2022.

BACKGROUND CONCERNING APPLE[2]

18. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

19. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email

---

[2] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased

through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

20. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

21. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

22. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

23. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

24. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents,

spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

25. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element of the TARGET OFFENSE. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation, such as the location of the crime and the identity of the perpetrators and any co-conspirators or aiders and abettors.

26. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device that connects to the Internet must use an IP address, IP address information can help

investigators understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

27. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

28. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify an account's user or users and/or co-conspirators, as well as additional evidence.

CONCLUSION

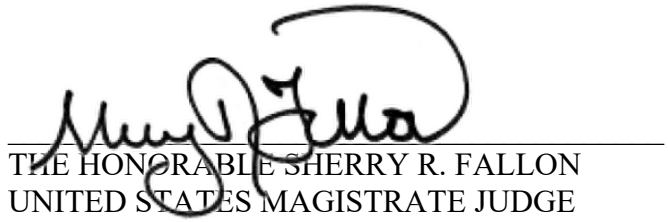
29. Based on the foregoing, I request that the Court issue the proposed search warrant.

30. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully Submitted,

/s/ Charles Neagle, Jr.
Charles A Neagle, Jr
Special Agent, Federal Bureau of Investigation

Sworn to me over the telephone and signed by me pursuant to Fed. R. Crim. P. 4.1 on this 13th day of April, 2022.



THE HONORABLE SHERRY R. FALLON
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with [redacted] (the "TARGET APPLE ID") that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at One Infinite Loop, Cupertino, California 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to the request made on April 11, 2022 under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. The contents of all instant messages associated with the TARGET APPLE ID from **April 3, 2022 through April 7, 2022**, including stored or preserved copies of instant messages (including WhatsApp messages, iMessages, SMS messages, and MMS messages) sent to and from the TARGET APPLE ID (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

b. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

c. All activity, connection, and transactional logs for the TARGET APPLE ID (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

d. All records and information regarding locations where the TARGET APPLE ID or devices associated with the TARGET APPLE ID were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps; and

e. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within fourteen (14) days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and/or instrumentalities of violations of the TARGET OFFENSE listed in the affidavit by suspects unknown to the investigators, from **April 3, 2022 through April 7, 2022**, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Evidence indicating the location of the device associated with the TARGET APPLE ID, including evidence indicating how and when the TARGET APPLE ID was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the TARGET APPLE ID user;

b. Evidence indicating the identity of the user of the TARGET APPLE ID as it pertains to the crime under investigation, including any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.